

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

**22 MAG 1337**

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Accounts



Maintained at  
Premises Controlled by Google LLC,  
USAO Reference No. 2021R00778

**TO BE FILED UNDER SEAL**

**AGENT AFFIDAVIT**

**Agent Affidavit in Support of Application for a Search Warrant  
for Stored Electronic Communications**

STATE OF NEW YORK     )  
  ) ss.  
COUNTY OF NEW YORK    )

, being duly sworn, deposes and states:

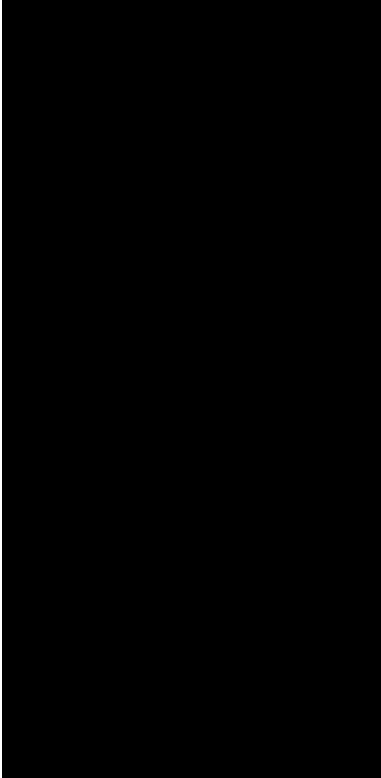
**I. Introduction**

**A. Affiant**

1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) for over two years. I have received training regarding the execution of search warrants and the conduct of investigations into public corruption and campaign finance crimes. I have participated in the execution of search warrants involving electronic evidence, including in investigations of public corruption and campaign finance crimes.

**B. The Provider, the Subject Account and the Subject Offenses**

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the following 11 email accounts:



(the “Subject Accounts”), maintained and controlled by Google LLC (the “Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of theft of federal funds and wire fraud, and conspiracy to commit the same, in violation of 18 U.S.C. §§ 371, 666, 1343, and 1349 (the “Subject Offenses”). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training

and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

### **C. Services and Records of the Provider**

4. I have learned the following about the Provider:

a. The Provider offers email services to the public. In particular, the Provider allows subscribers to maintain email accounts under any domain name under the subscriber's control. For example, if a subscriber controls the domain name "xyzbusiness.com," the Provider enables the subscriber to host any email address under this domain name (e.g., "john@xyzbusiness.com"), on servers operated by the Provider. A subscriber using the Provider's services can access his or her email account from any computer connected to the Internet.

b. The Provider maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Provider's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the the Provider's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for a certain period of time.

ii. *Subscriber and billing information.* The Provider collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, recovery and alternate email addresses,

and sign-in phone numbers. A recovery email address, which can be associated with more than one Gmail account, is used to regain access to an account if a password has been forgotten or a user has been locked out of their account. An alternate email address is a non-Gmail account that a user has provided that can be used to sign into a Gmail account. A sign-in phone number is a phone number that can be used as a primary/additional login identifier to access an account. The Provider also maintains records concerning the date on which the account was created, the Internet protocol (“IP”)<sup>1</sup> address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of The Provider services utilized by the subscriber. Finally, the Provider maintains records regarding (1) fetching and forwarding email addresses, which are email accounts from which the primary account receives emails and forwards emails, respectively; (2) email aliases, domain aliases or separate domains associated with the account, which are means by which accounts with other domain names or other email addresses can be associated with a primary the Provider account; (3) other the Provider accounts that have access to the primary account, which access can be granted by the user of the primary account; and (4) other email accounts that are associated with the primary the Provider account.

iii. *Device Information.* The Provider may also collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers

---

<sup>1</sup> Based on my training and experience, each electronic device connected to the Internet must be assigned a unique IP address so that communications from or directed to that electronic device are routed properly.

(“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

iv. *Cookie Data.* The Provider typically uses features to track the activity of users of its accounts, including whether or not the user of an account accesses other accounts at the Provider using the same computer or device, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by The Provider when a computer visits its site or logs into an account.

v. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system, including records of login and logout events relating to the Provider accounts, including user IP addresses and dates and timestamps.

vi. *Customer correspondence.* The Provider also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

vii. *Preserved and backup records.* The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

#### **D. Jurisdiction and Authority to Issue Warrant**

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the

Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

## **II. Probable Cause**

### **A. Probable Cause Regarding the Subject Offenses**

8. Since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York and have been investigating the possible receipt of so-called “straw” donations by the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”). A straw, or “conduit,” donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person.

9. I understand, based on my review of publicly available information, that:

a. The Adams Campaign accepted matching funds from the New York City Campaign Finance Board throughout a significant part of its campaign (“Matching Funds”),

meaning that the Adams Campaign received funds from the New York City government as a result of donations the Adams Campaign received from private donors.<sup>2</sup>

b. Under New York City law, the Adams Campaign was eligible to receive \$2,000 in Matching Funds, and no more than \$2,000 in Matching Funds, for each donation of \$250 from an individual donor who resides within New York City. If an individual donated more than \$250, any amount in excess of \$250 would not be eligible for matching funds.<sup>3</sup>

c. New York City receives in excess of \$10,000 per year in federal funding.<sup>4</sup>

10. I understand, based on publicly available material posted to the Internet, such as corporate websites of firms involved in the construction industry, as well as campaign contribution forms provided by the New York City Campaign Finance Board, and information provided by the Provider in response to an order under 18 U.S.C. § 2703(d), that each of the Subject Accounts is used by an officer or employee (the “Subjects”) of [REDACTED], a New York State corporation that operates in the construction industry in New York City. For example, the Subject Account [REDACTED] is used by Subject Erden Arkan, who is the owner of [REDACTED].

<sup>2</sup> See, e.g., <https://www.ny1.com/nyc/all-boroughs/news/2021/10/08/eric-adams-is-taking-a-rare-step--turning-down-campaign-cash> (reporting on the Adams Campaign’s prior acceptance of matching funds and decision to turn down some matching funds as of October 7, 2021); [https://www.nycfb.info/VSAppe/CandidateSummary.aspx?as\\_cand\\_id=1545&as\\_election\\_cycle=2021&cand\\_name=Adams%2C+Eric+L&office=Mayor&report=summ](https://www.nycfb.info/VSAppe/CandidateSummary.aspx?as_cand_id=1545&as_election_cycle=2021&cand_name=Adams%2C+Eric+L&office=Mayor&report=summ) (New York City Campaign Finance Board’s report detailing total public funds disbursed to Adams Campaign).

<sup>3</sup> See <https://www.nycfb.info/program/how-it-works>.

<sup>4</sup> See [https://comptroller.nyc.gov/wp-content/uploads/2016/11/Federal\\_Budget\\_Vulnerabilities\\_Memo.pdf](https://comptroller.nyc.gov/wp-content/uploads/2016/11/Federal_Budget_Vulnerabilities_Memo.pdf)

11. I understand, based on contribution forms provided by the New York City Campaign Finance Board, that the Adams Campaign received the following donations, among others, on May 7, 2021:

| AMOUNT  | NAME         | CITY           | STATE | OCCUPATION         | EMPLOYER NAME |
|---------|--------------|----------------|-------|--------------------|---------------|
| \$1,500 | Arkan, Erden | New York       | NY    | Owner              | [REDACTED]    |
| \$1,200 | [REDACTED]   | Flushing       | NY    | Sr. Manager Prod.  | [REDACTED]    |
| \$1,250 | [REDACTED]   | Brooklyn       | NY    | Account Manager    | [REDACTED]    |
| \$1,250 | [REDACTED]   | Flushing       | NY    | Construction       | [REDACTED]    |
| \$1,250 | [REDACTED]   | Cliffside Park | NJ    | Business Logistics | [REDACTED]    |
| \$1,250 | [REDACTED]   | Brooklyn       | NY    | PM                 | [REDACTED]    |
| \$1,250 | [REDACTED]   | Brooklyn       | NY    | Engineer/Lawyer    | [REDACTED]    |
| \$1,250 | [REDACTED]   | Brooklyn       | NY    | Project manager    | [REDACTED]    |
| \$1,250 | [REDACTED]   | Ridgewood      | NJ    | Finance Director   | [REDACTED]    |
| \$1,250 | [REDACTED]   | Flushing       | NY    | Partner            | [REDACTED]    |
| \$1,250 | [REDACTED]   | New York       | NY    | Accountant         | [REDACTED]    |

<sup>5</sup> The description of [REDACTED] as an “Engineer/lawyer” at [REDACTED] is taken from the donation form submitted to the New York City Campaign Finance Board as part of her donation, but it appears from publicly available information that [REDACTED] may not in fact be employed at [REDACTED], although as explained in ¶ 12, her husband does appear to be employed at [REDACTED].



All of the donors in the above table are Subjects, except that [REDACTED] is not a Subject for reasons explained in the following paragraph.

12. Bank records for [REDACTED] indicate that on April 28, 2021, [REDACTED] issued checks in the amount of \$1,250 to each of the Subjects with the exception of [REDACTED] and Arkan, and also issued a \$1,250 check to [REDACTED], who I know from law enforcement databases is [REDACTED] spouse. Put another way, on April 28, 2021, [REDACTED] paid each of the donors to the Adams Campaign listed above in ¶ 11 the amount of their May 7, 2021 donation, with the exceptions of [REDACTED] whose husband instead received a check for that amount, Arkan, who as noted above is the owner of [REDACTED], and [REDACTED] who donated \$50 less to the Adams Campaign than [REDACTED] received from [REDACTED].<sup>6</sup> For the foregoing reasons, [REDACTED] is also a Subject. Based on information from a publicly available website that provides information on holders of certain visas and a publicly available construction industry website, I believe that [REDACTED] is employed by [REDACTED], where [REDACTED] email address is [REDACTED] which is one of the Subject Accounts.

13. Toll records indicate that on May 19, 2021, a phone number subscribed to by [REDACTED] [REDACTED] and a phone number subscribed to by Arkan exchanged two calls, one of which resulted in a call of one minute and 11 seconds duration and the other of which did not result in a listed duration (possibly indicating that the call was not answered). I know from my review of media reports, among other sources, that [REDACTED] is a longtime advisor of Eric Adams who worked in the Special Counsel's office of the Brooklyn Borough President when Adams was Brooklyn

---

<sup>6</sup> In its prior request to this Court for an order under 18 U.S.C. § 2703(d), the Government erroneously stated that all of the apparent reimbursements from [REDACTED] were for \$50 more than the Subjects (or their spouse, in [REDACTED] case) had donated to the Adams Campaign. In fact, only [REDACTED] donated \$50 less than the check [REDACTED] issued to [REDACTED]. This error resulted from a misreading of the underlying records by other FBI personnel, but I have personally reviewed the records in question and the statements above in ¶ 12 are now correct.

Borough President and now works in the International Relations Department of New York City Hall.

**B. Probable Cause Regarding the Subject Accounts**

14. I believe that each of the Subject Accounts is used by a Subject listed in the table above in ¶ 11 because, as discussed above, publicly available information and/or campaign contribution forms associate the email addresses with the Subjects, and each of the Subject Accounts consists of a Subject's last name and the [REDACTED] domain name.

15. I have reviewed records provided by the Provider in response to a court order issued under 18 U.S.C. § 2703(d), which reflect the header information for emails sent to and from each of the Subject Accounts, among other email accounts.<sup>7</sup> From that information I know, among other things, that in total there were at least 1,059 emails between the Subject Accounts—meaning emails on which at least one Subject Account was the sending account and at least one Subject Account was the receiving account—between April 15, 2021 and May 15, 2021. Among those emails, I have observed several exchanges involving many Subject Accounts at around the time of the apparent straw donations described above. For example, on or about May 7, 2021, one of the Subject Accounts sent an email on which all of the remaining Subject Accounts were recipients; and on or about May 5, 2021, one of the Subject Accounts sent an email on which nine of the remaining 10 Subject Accounts were recipients, which led to a further exchange of emails involving many of the Subject Accounts.

---

<sup>7</sup> The § 2703(d) order directed the Provider to provide information for each of the Subject Accounts except the account [REDACTED], which the FBI had not identified at the time the 2703(d) order was requested. Because, however, the account [REDACTED] exchanged emails with other Subject Accounts that were named in the order and for which I was therefore able to review data, the statements in ¶ 15 also apply to that account.

16. Based on my training and experience, I know that individuals with access to email who are conducting criminal activity, like any other organizational activity, often communicate using email accounts like the Subject Accounts. This is particularly true where, as here, the participants are members of the same corporation or organization and are in the habit of regularly communicating with each other using electronic mail.

17. Temporal Limitation. This application is limited to all content created, sent, or received on or after April 1, 2021 through November 2, 2021, which runs from the month in which the funds for the possible straw donations were sent to the Subjects until the close of the 2021 election in which the Adams Campaign participated.

### **C. Evidence, Fruits and Instrumentalities**

18. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

### **III. Review of the Information Obtained Pursuant to the Warrant**

19. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and

instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

20. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

#### **IV.Request for Non-Disclosure and Sealing Order**

21. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. As is set forth above in Paragraphs 11 to 16, the Subjects are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital

evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3).

22. Accordingly, there is reason to believe that, were the Provider to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

23. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.


24. Finally, based on my training and experience, I know that the Provider will request that the Government seek data related to an enterprise such as [REDACTED], which would include data relating to the Subject Accounts, directly from the enterprise, pursuant to the U.S. Department of Justice Policy titled Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, available at <https://www.justice.gov/criminal-ccips/file/1017511/download>. However, pursuant to that policy, because [REDACTED] appears to be controlled by one the Subjects of this investigation and closely associated with other Subjects (as set forth above) who would be in a position to delete, encrypt, or otherwise conceal the requested data if alerted to the Government's investigation, I respectfully request that the proposed order specifically require the Provider to produce enterprise data.

**V. Conclusion**

25. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

██████████ by the Court, with permission  
██████████  
Special Agent  
Federal Bureau of Investigation

Sworn to me through the transmission of this  
Affidavit by reliable electronic means, pursuant to  
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, this  
9th of February, 2022 (FaceTime)

  
\_\_\_\_\_  
HONORABLE DEBRA FREEMAN  
United States Magistrate Judge  
Southern District of New York

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Accounts



Maintained at  
Premises Controlled by Google LLC,  
USAO Reference No. 2021R00778

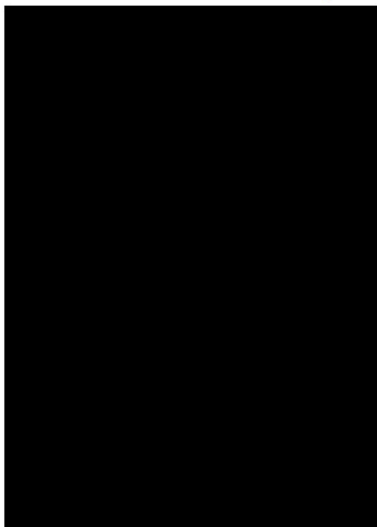
**22 MAG 1337**

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Google LLC ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

**1. Warrant.** Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts:





(the “Subject Accounts”), maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. Based on the affidavit’s representation that an enterprise whose data is sought pursuant to this warrant appears to be controlled by and closely associated with the targets of the Government’s investigation, the Provider is specifically directed to produce data for any enterprise accounts responsive to this Warrant. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider



may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

2/9/2022  
Date Issued

1:49 p.m.  
Time Issued

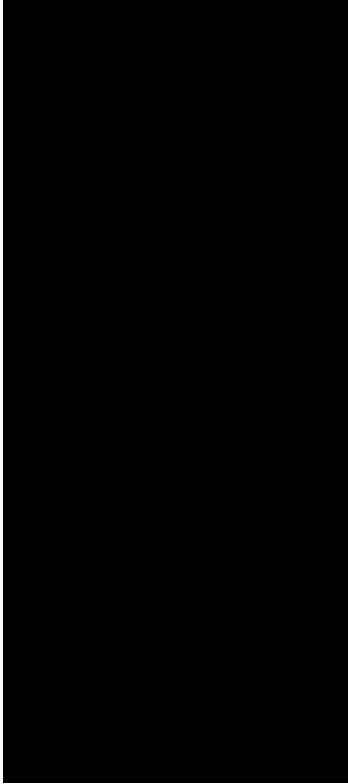


UNITED STATES MAGISTRATE JUDGE  
Southern District of New York

## **Email Search Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Google LLC (the “Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email accounts



(the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

## II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between April 1, 2021 and November 2, 2021, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

### III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of theft of federal funds and wire fraud, and conspiracy to commit the same, in violation of 18 U.S.C. §§ 371, 666, 1343, and 1349, including the following:

- a. Evidence relating to coordination among employees, officers, and associates of [REDACTED] concerning political contributions to the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”).
- b. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making political contributions to the Adams Campaign.
- c. Evidence of the motive or purpose of political contributions to the Adams Campaign by employees, officers, and associates of [REDACTED].
- d. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] for political contributions to the Adams Campaign.
- e. Evidence relating to coordination or communication between the Adams Campaign and employees, officers, and associates of [REDACTED], or persons paying employees, officers, and associates of [REDACTED] for political contributions to the Adams Campaign.
- f. Evidence of other individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.
- g. Evidence of intent to make unlawful political contributions or violate the campaign finance laws.

h. Evidence of knowledge of the campaign finance laws, including but not limited to knowledge of the prohibition of making contributions in the name of another person.

i. Passwords or other information needed to access user's online accounts.